STRATEGIE NATIONALE VEILIGHEID

-BEVINDINGENRAPPORTAGE-

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Risico's en onzekerheden zijn niet uit te sluiten; 100% veiligheid bestaat niet. Ons land kan op talloze manieren worden bedreigd, bijvoorbeeld door natuurgeweld, technisch of menselijk falen, maar ook door mensen of groepen die opzettelijk schade of letsel willen berokkenen of criminele intenties hebben. De nationale veiligheid kan bedreigd worden op Nederlands grondgebied of ten aanzien van Nederlandse belangen in het buitenland.

De nationale veiligheid is in het geding als de vitale belangen van Nederland en de Nederlandse staat in gevaar zijn. Deze vijf vitale belangen zijn: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid en sociale en politieke stabiliteit. De strategie Nationale Veiligheid (strategie NV) is er op gericht aantasting van deze vitale belangen, die mogelijk kunnen leiden tot maatschappelijke ontwrichting, zoveel mogelijk te voorkomen.

1.2 Bouwstenen Strategie Nationale Veiligheid

De werkwijze van deze strategie maakt het mogelijk om een breed en divers palet aan mogelijke risico's in kaart te brengen en onderling te vergelijken, en op basis daarvan keuzes te maken voor te nemen maatregelen.

Het in het kader van de strategie NV ontwikkelde risicodiagram helpt bij het visualiseren van deze risicovergelijking (zie hoofdstuk 2). Het vergelijken van de risico's kan vervolgens helpen bij het maken van afwegingen en keuzes voor te nemen maatregelen ter verbetering. Waar gaan we nu direct mee aan de slag, wat kan later en wat doen we niet? Dat zijn politieke vragen die in de strategie NV elk jaar weer beantwoord moeten worden.

De kern van de strategie NV bestaat uit drie onderdelen:
1. de Nationale Risicobeoordeling (NRB);
2. de capaciteitenanalyses;
3. de bevindingenrapportage Nationale Veiligheid (het voorliggend document).

Ad 1. NRB
In het eerste onderdeel van de strategie NV, de *NRB*[1]*,* wordt elk jaar een beperkt aantal risico's geanalyseerd die op Nederland kunnen afkomen en waarvan vermoed wordt dat ze maatschappelijk ontwrichtend kunnen zijn. Dit kunnen risico's zijn die nog niet eerder onderzocht zijn of waarbij zich nieuwe feiten of inzichten voordoen. De risico's worden uitgewerkt tot scenario's[2]. Deze scenario's worden vervolgens door experts op twee punten beoordeeld. Ten eerste beoordelen de experts op tien impactcriteria, die de vijf vitale belangen kenmerken. Ten tweede schatten de experts in hoe groot de waarschijnlijkheid is dat de scenario's werkelijkheid worden. De gebruikte methodiek van

[1] De tekst van de NRB is te downloaden op www.nctv.nl
[2] Gedachtenexperiment hoe risico's zich zouden kunnen ontwikkelen tot een daadwerkelijk incident/ramp met als gevolg maatschappelijke ontwrichting. Het zijn nadrukkelijk geen voorspellingen.

scenarioanalyse en beoordeling (scoring) maakt het mogelijk om ook onzekere risico's (risico's waarbij theoretische en/of empirische wetenschappelijke gegevens over waarschijnlijkheid en impact slechts beperkt beschikbaar zijn) te analyseren.

In 2011 is de NRB voor het eerst uitgevoerd door experts vanuit het speciaal hiervoor opgerichte analistennetwerk nationale veiligheid (ANV)[3]. Met de oprichting van dit netwerk is een belangrijke stap gezet in het versterken van de strategie NV. Het netwerk moet zorgen voor het efficiënt ontsluiten van benodigde kennis voor het uitvoeren van scenarioanalyses. De kennis en kunde van een aantal gerenommeerde kennisinstituten en inlichtingendiensten vormen de kern van dit netwerk. Het netwerk moet bijdragen aan het verder ontvlechten van enerzijds de scenarioanalyse door inhoudsdeskundigen en anderzijds doorvertaling in beleidsconsequenties door de verantwoordelijke ministeries.

Ad 2. Capaciteitenanalyses
In het tweede onderdeel worden aan de hand van de resultaten uit de NRB capaciteitenanalyses uitgevoerd. Dit zijn analyses waarbij in beeld wordt gebracht in hoeverre de maatschappij is voorbereid op het voorkomen van incidenten enerzijds en het beperken en beheersen van de impact van mogelijke incidenten anderzijds, zoals in de scenario's beschreven.
Op basis van de uitkomsten van deze capaciteitenanalyses wordt een integrale afweging gemaakt welke capaciteiten[4] versterkt zouden moeten worden om de beschreven risico's te reduceren, en dus onzekerheden beter hanteerbaar te maken. Deze capaciteiten zijn of specifiek van aard (gericht op één risico) of breed inzetbaar (toepasbaar bij het beperken van meerdere risico's). Ook de capaciteitenanalyse wordt uitgevoerd op basis van een vooraf vastgestelde systematiek.

Ad 3. Bevindingenrapportage
Als laatste wordt de bevindingenrapportage geschreven. Uit de afzonderlijke capaciteitenanalyses wordt in overleg tussen de verantwoordelijke ministeries een selectie gemaakt uit de door de deskundigen geprioriteerde capaciteiten. Hierbij wordt gelet op onder meer doelmatigheid en toegevoegde waarde in vergelijking met eerder vastgestelde capaciteiten. Deze capaciteiten worden vervolgens door de ambtelijke Stuurgroep Nationale Veiligheid aan het kabinet ter besluitvorming voorgedragen. Het kabinet beslist uiteindelijk op basis van de bevindingenrapportage welke aanbevelingen worden uitgevoerd.

---

[3] Het analistennetwerk nationale veiligheid wordt gevormd door een consortium bestaande uit een zestal kennisinstellingen (RIVM, AIVD, WODC, TNO, Clingendael, ISS/EUR). Ten behoeve van de te maken analyses wordt door dit consortium extra kennis en expertise ingeroepen van kennisdragers in de wetenschap, overheid en bedrijfsleven. Kerntaak van het consortium is scenarioanalyses op het terrein van de nationale veiligheid in het algemeen en met name de Nationale Risicobeoordeling in het bijzonder uit te voeren.

[4] Een capaciteit is het vermogen van de (rijks)overheid en private partners om taken uit te voeren die (mede) tot doel hebben de nationale veiligheid te beschermen. Het gaat hierbij om bepaalde combinaties van middelen (bijv. materiaal of informatie-systemen), mensen (civiel, militair, et cetera) en methoden (zoals procedures, plannen, oefenen, PPS-verbanden). Capaciteiten helpen de kans en/of de impact van een of meerdere dreigingen te reduceren. Capaciteiten kunnen het totale spectrum van preventie, preparatie, respons, repressie en nazorg beslaan.

1.3 Resultaten van de Strategie

De Strategie nationale veiligheid wordt sinds 2008 door het kabinet gebruikt. Ten behoeve hiervan zijn inmiddels 42 scenario's ontwikkeld en zijn ook nog eens vijf scenario's geactualiseerd. Op basis van deze scenario's zijn capaciteitenanalyses uitgevoerd en heeft het kabinet te versterken capaciteiten geïdentificeerd. Het verbeteren van bepaalde capaciteiten heeft altijd tot doel om de weerbaarheid tegen mogelijke risico's te vergroten of om de impact te verkleinen in het geval een dergelijk scenario zich toch voordoet. Het merendeel van deze capaciteiten is opgepakt en inmiddels afgerond; een aantal capaciteiten is ook onderdeel geworden van het continue proces, te denken valt dan bijvoorbeeld aan de 'integrale cyber dreigings- en risicoanalyse' of 'Strategisch overleg met Duitsland, Frankrijk en Groot-Brittannië'. Onderstaande tabel is een overzicht van alle sinds 2008 te versterken capaciteiten.

Te versterken capaciteit	**Status**
Landelijke strategieën voorbereiding voor de verdeling van schaarse middelen	In uitvoering
EU oliecrisis richtlijn	Afgerond
Nationaal crisisplan energie	In uitvoering
Met voorrang opstellen landelijk evacuatieplan	Afgerond
Onderzoeken mogelijkheden opzetten landelijk operationele staf voor nationale crisis	Afgerond
Doorlichting IVenJ op Intensivering Civiel Militaire Samenwerking	Afgerond / Continu proces
Landelijk systeem voor uniforme informatievoorziening en –uitwisseling tussen alle niveaus en bestuurlijke en functionele kolommen (Netcentric)	Continu proces
Robuustheid communicatiemiddelen	Afgerond
Zelfredzaamheid en burgerparticipatie	Afgerond
Nationaal crisisplan griepepidemie	Afgerond
Continuïteit vitale infrastructuur inzichtelijk maken	Afgerond
Analyseren effecten van internationale schaarste	Afgerond
Evaluatie oliecrisismechanismen	Afgerond
Nationale Risico Beoordeling op Europese agenda	Afgerond
Nationaal crisisplan opstellen	Vervallen omdat blijkt dat Nationaal handboek crisisbesluitvorming voldoet
Strategisch overleg Duitsland, Frankrijk en Groot Brittannië	Afgerond / Continu proces
Versterken van de weerbaarheid van vitale sectoren tegen de uitval van elektriciteit en ICT	In uitvoering
Daadkrachtig leiderschap bij crisis bijeenkomstenserie	Afgerond
Toetsingskader nationale crisisorganisatie ontwikkelen	Afgerond
Valideren van huidige structuur en systeem kernongevallenbestrijding	In uitvoering

Vernieuwde crisiscommunicatie op regionaal niveau	Continu proces
Inrichten van rijksbrede informatieloketfunctie	Afgerond
Koppeling Nationale Risicobeoordeling en regionale risicoprofielen en capaciteitsplanning nationaal en regionaal niveau	Afgerond
Maatregelen aanpak verwevenheid onder en bovenwereld	Continu proces
Opstellen nationaal crisisplan ICT	Afgerond
Integriteit (handvatten burgemeesters, wethouders en raadsleden)	Afgerond
NL Alert	Afgerond / continu proces
Versterking Rechterlijke Macht	Afgerond
Planvorming en informatie-uitwisseling/kennisdeling tussen Veiligheidsraad en VenJ verbeteren	Afgerond
Oprichten ICT responsboard	Afgerond
Oprichten van expertpoule	In uitvoering
Oprichten kenniscentrum politie	In uitvoering
Versterken van de politieorganisatie	Afgerond / continu proces
Continuïteitsplannen voor uitval van ICT en elektriciteit	In uitvoering
Regio's ondersteunen in hun rol op het gebied van zelfredzaamheid	Afgerond
Strategisch topoverleg VNO/NCW	Afgerond / continu proces
Integrale cyber dreigings- en risicoanalyse	Afgerond / continu proces
Europese infrastructuren sector energie en transport van vitaal belang voor Nederland	In uitvoering
Implementatie kabinetsreactie Kwetsbaar-heidsanalyse Spionage Nederland	Continu proces
Versterken rol bestuurders bij crisiscommunicatie	In uitvoering
Kabinetsvoorstel over versterking van de regierol bij de rijksoverheid	Afgerond
Vergroten weerbaarheid vitale infrastructuur tegen ICT-dreigingen en cyberaanvallen	Afgerond
Inventarisatie van kritische grondstoffen die NL in belangrijke mate uit het buitenland haalt en die van cruciaal belang zijn voor de economie	Afgerond
Kabinetsoefening	Afgerond / continu proces
Oprichten cybersecurityraad	Afgerond
Nationale Cyber Security Strategie plus actieplan	Afgerond
Versterking samenwerking nationaal/regionaal bij crisiscommunicatie	In uitvoering
Versterking crisiscommunicatie op nationaal niveau	Afgerond
Aanpak eenlingen	Continu proces
Vergroten weerbaarheid tegen gevolgen satellietuitval door zonnestormen	In uitvoering

Convenanten veiligheidsregio's en vitale sectoren	Continu proces
Versterken van detectie van aanvallen op netwerken en informatiesystemen	Continu proces
Het vermogen om (potentiële) sociale calamiteiten effectief te beheersen	In uitvoering

1.4 Leeswijzer

In hoofdstuk 2 worden de belangrijkste uitkomsten van de NRB 2012 kort beschreven. In hoofdstuk 3 wordt het advies gepresenteerd voor de te versterken capaciteiten (specifiek en breed inzetbaar), op basis van de uitkomsten van de capaciteitenanalyses.

2 Toelichting op de Nationale Risicobeoordeling 2012

2.1 Inleiding

De start van de strategie NV ligt, zoals ook al in de inleiding aangegeven, bij de realisatie van de jaarlijkse nationale risicobeoordeling (NRB), in dit geval de NRB over het jaar 2012 waar in dit hoofdstuk uitgebreider op wordt ingegaan.

2.2 Totstandkoming NRB 2012

De scenario's zijn onafhankelijk geproduceerd door het Analistennetwerk Nationale Veiligheid (ANV). Het ANV is een gezaghebbend kennisnetwerk dat sinds 2011 in opdracht van het ministerie van Veiligheid en Justitie, namens de Stuurgroep Nationale Veiligheid (SNV), jaarlijks de NRB opstelt. De ambtelijke stuurgroep Nationale Veiligheid heeft voor de NRB 2012 vier dreigingstypen geselecteerd, die door het ANV zijn uitgewerkt tot in totaal vier scenario's. Het gaat om de volgende scenario's:

Digitale veiligheid: "Cyberhacktivisme"
Terrorisme: "Gewelddadige eenling"
Internationale vraagstukken: "Wapenbeheersing falende staat"
Sociale onrust: "Grootschalige onlusten"

Hierna volgt een korte beschrijving van de belangrijkste inzichten uit de NRB 2012[5].

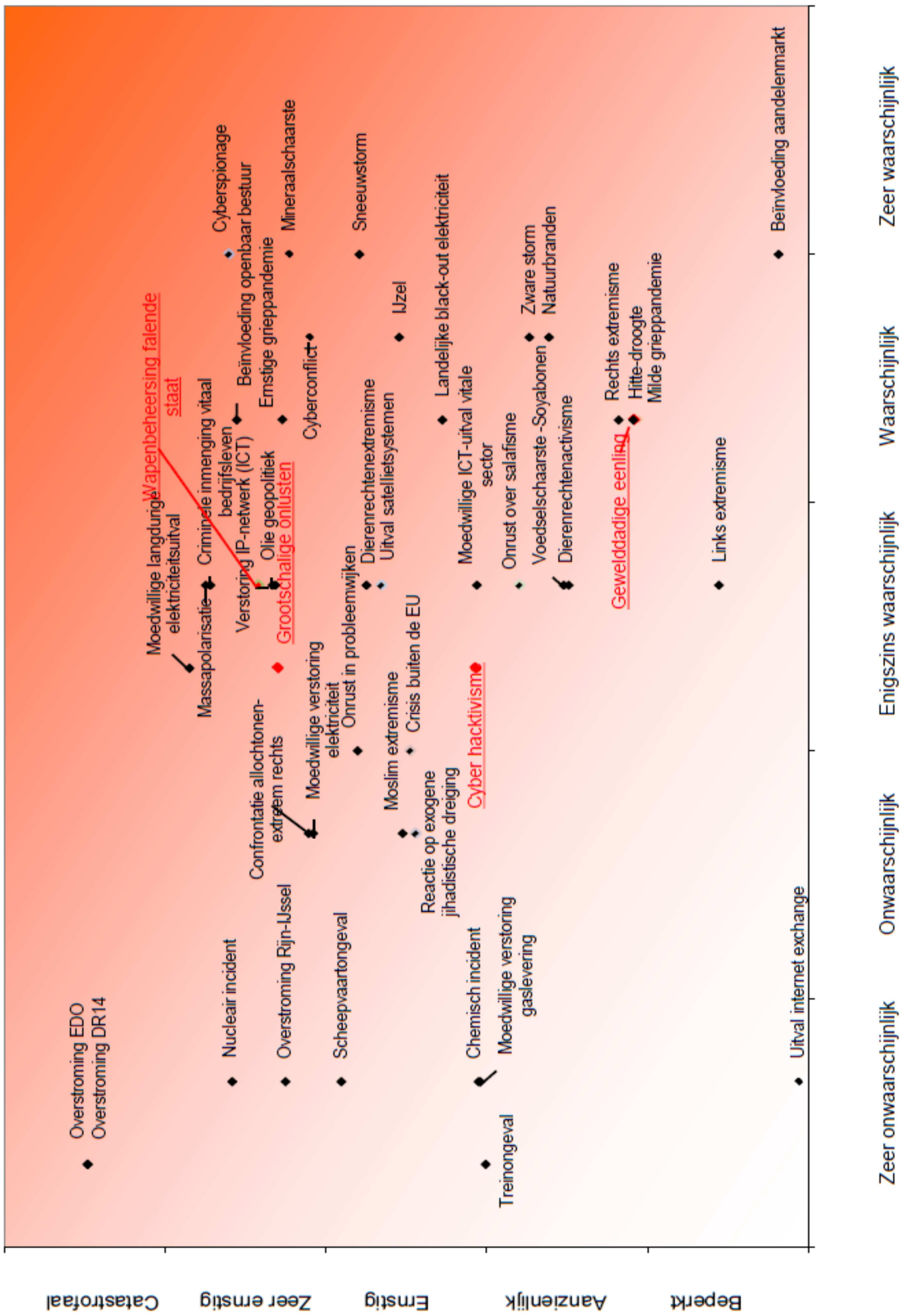
2.3 De plaats van de nieuwe scenario's in het risicodiagram

Hoe het risicodiagram te lezen?
De resultaten van de risicobeoordeling door de experts zijn voor elk scenario grafisch weergegeven in het risicodiagram (figuur 1.1). De scenario's zijn door experts beoordeeld op een tiental impactcriteria en geschat is hoe groot de kans is dat de scenario's werkelijkheid worden.

In dit diagram heeft elk scenario een positie op grond van de door de experts geschatte waarschijnlijkheid (horizontale as) en impact (verticale as). Bij elkaar vormt dit de relatieve risicopositie van een scenario. De scenario's die in 2012 zijn ontwikkeld zijn met een rode kleur en onderstreept weergegeven. De scenario's uit reeds eerder uitgevoerde NRB's zijn in zwart weergegeven.
Het is van belang te realiseren dat deze scoring betrekking heeft op het specifieke scenario en dus niet op het brede fenomeen.

[5] De tekst van de NRB is te downloaden op www.rijksoverheid.nl

Figuur 1.1: Risicodiagram



Overwegingen bij de NRB en het risicodiagram
Van alle mogelijke scenario's die voor een bepaald risico kunnen worden gemaakt, worden er in de NRB steeds één of slechts enkele uitgewerkt. Voor de meeste scenario's is immers ook een ernstiger variant denkbaar, of juist een minder ernstige. Of varianten met andere eigenschappen, een ander verloop, in andere omstandigheden of een andere context. Gekozen wordt voor die scenario's die inzicht geven in de capaciteiten die nodig zijn om de beschreven risico's het hoofd te bieden.

Daarnaast worden de meeste risico's waar de strategie NV zich op richt gekenmerkt door een zekere mate van onzekerheid: het gaat om gebeurtenissen die weinig voorkomen (en waar dus weinig empirische gegevens van zijn) en om scenario's die complex zijn (waar dus veel elementen een rol spelen waarvan de onderlinge samenhang niet altijd bekend is. Daardoor kan het gebeuren dat de individuele risicobeoordelingen van de experts variëren binnen een bepaalde bandbreedte. In het risicodiagram zijn steeds middenwaardes van de expertscores weergegeven.

2.4 Belangrijkste uitkomsten nieuwe scenario's

In deze paragraaf wordt per nieuw scenario kort ingegaan op de uitkomsten. Verder wordt ingegaan op de positie van het scenario in het risicodiagram.

Scenario Cyberhacktivisme
Dit scenario speelt in een wereld waarin regelmatig protestacties vanuit de hackerswereld worden gehouden door onder andere internationaal opererende hactivistische groepen als Ahackgroup. Er zijn politieke spanningen in Europa door teruglopende economie en een hoge (jeugd)werkloosheid. Gedreven door een teruglopende economie gaan bedrijven steeds vaker over op uitbesteding van informatie- en communicatietechnologie (ICT) tegen de laagst mogelijke kosten, gebruikmakend van cloudoplossingen. Eind 201X zijn enkele duizenden technisch hoogopgeleide ICT-beheerders en systeemprogrammeurs 'in between jobs'. Een aantal van hen organiseert onder de naam Ontevredenen maandelijks een denial-of-service protestactie. Het NCSC heeft van de AIVD gehoord dat de harde kern van Ontevredenen mogelijk aansluiting zoekt bij Ahackgroup, een internationaal bekende hacktivistische groepering.

De federale overheid van de Verenigde Staten is in maart 201X wederom overvallen door een golf van gelekte overheidsinformatie. De aan Ahackgroup gelieerde klokkenluiderssite Kickbacks toont gelekte documenten en heimelijk opgenomen filmpjes van omkopingen van senatoren en topambtenaren in de VS door zogenaamde lobbyisten uit Westerse en andere landen. Voordat de documenten op Kickbacks geplaatst zijn, zijn ze door een internationale groep van elkaar vertrouwende internetjournalisten en ex-hackers getoetst op echtheid en gescreend op veiligheidsaspecten. Dat laatste is noodzakelijk omdat een aantal omkoop-documenten over zwarte defensieprogramma's van de Verenigde Staten en de Five Eyes landen gaat. Op deze wijze wil Kickbacks het lekken van staatsgeheimen voorkomen. Tot de internationale toetsgroep behoren drie prominent bekendstaande Nederlandse hackers van het eerste uur. Justitie ontvangt medio oktober 201X een rechtshulpverzoek met de vraag om uitlevering van dit drietal.

Zij worden verdacht van het verduisteren en publiek maken van Amerikaanse staatsgeheimen en andere gevoelige informatie. Justitie bestudeert het verzoek en gaat de mogelijke (inter)nationale juridische belemmeringen na.

In dezelfde periode kondigt salarisverwerker XSP aan dat zij per direct haar Nederlandse computercentra sluit. Van daaruit worden ruim 1,7 miljoen salarisstrookjes per maand voor vele duizenden Nederlandse bedrijven verstuurd. De werkgelegenheid van enkele honderden ICT-ers gaat daarmee verloren.

Dan volgt een aantal ontwikkelingen elkaar snel op. Op maandag 18 december, terwijl de temperaturen ver onder het nulpunt schieten en een Elfstedentocht in aantocht is, worden de drie verdachte hackers opgepakt door de politie. Nadat het OM de reden hiervan heeft toegelicht buitelen de nieuwsmedia over elkaar heen, maar worden ook de activistische groepen actief als tegenreactie. Burgers worden opgeroepen om de internetvrijheid te verdedigen door cyberaanvallen tegen de Nederlandse overheid en de rechtse media uit te voeren. Voor middelen wordt verwezen naar enkele underground sites.
Diverse hackersgroepen vallen ongecoördineerd websites aan.

Nieuw is dat ook industriële controlesystemen worden aangevallen. Zo worden printerbestanden voor melkproductverpakkingen gehackt en voorzien van de boodschap "Laat ze vrij". Ook wordt de verkaste salarisbetaler XSP aangevallen. De luchtbehandelingssystemen in diverse buitenlandse vestigingen worden tegelijk gesaboteerd. Apparatuur en schijfeenheden raken daardoor defect. Bij gebrek aan een businesscontinuïteitsplan zal het drie tot vijf dagen zal duren voordat de salarissen overgemaakt zullen worden.

Ahackgroup meldt dat Nederland zal worden gestraft voor de arrestaties. De drie gearresteerden moeten onmiddellijk vrijgelaten worden. Ahackgroup claimt dat een eerste slag aan Nederland is toegebracht. Er zullen er meer volgen. Terwijl de eerste kamervragen worden gesteld treedt de nationale crisisbesluitvormingsstructuur in werking. Op aangeven van de Nationaal Coördinator Terrorismebestrijding en Veiligheid wordt na ministerieel overleg de ministeriële commissie Crisisbeheersing bijeengeroepen. De ICT Respons Board (IRB) wordt geactiveerd.

Terwijl het buiten steenkoud blijft, volgen de gebeurtenissen elkaar snel op. E-thermostaten worden gehackt. De stoomleiding in de Korte Hoogstraat te Rotterdam barst als gevolg van gehackte IACS waardoor tientallen slachtoffers vallen met ernstige brandwonden. Ahackgroup claimt de verantwoordelijkheid. Ook raken hydrofoorinstallaties en luchtbehandelingen in verschillende psychiatrische inrichtingen en ouden-van-dagen-tehuizen in Nederland van slag. Een combinatie van de gladheid, gebrek aan capaciteit zorgt voor een langdurige herstelperiode.

Binnen de IRB-structuur wordt de conclusie getrokken dat er nog steeds geen vitale infrastructuur geraakt is of in gevaar is. De cyberverstoringen zijn nog steeds beheersbare lokale incidenten dan wel in het buitenland. Uit voorzorg wordt wel een 24-uursbezetting van het NCSC ingesteld en schalen ook de bedrijven hun veiligheidsmaatregelen op.

Het NCSC constateert dat de internationale media-aandacht leidt tot een toename van geautomatiseerde cyberaanvallen (Distributed denial of service oftewel DDoS, en poortscanning) en meer professionele hackpogingen op zowel systemen van de overheid als de vitale infrastructuur. De bronnen van deze DDoS-aanvallen lijken in de Zuid-Europese landen te liggen. Ook krijgen de website en telefoonlijnen van het NCSC last van DoS-aanvallen.
Zowel vitale als niet-vitale bedrijven komen onder vuur te liggen van hackersgroepen. Waar aanvallen op de goed beschermde vitale bedrijven mislukken, worden niet-vitale bedrijven hard geraakt. Een kleine chemische fabriek explodeert, waardoor twee woonwijken voor enkele dagen geheel geëvacueerd moeten worden. De hackers dreigen met meer cyberaanvallen op Nederland, tenzij de drie onmiddellijk worden vrijgelaten. Voor drie multinationals die in het Amerikaanse omkoopschandaal genoemd worden, wordt 'hoge dreiging' voor door IACS bestuurde processen afgekondigd. De IRB adviseert extra alertheid voor de vitale infrastructuren. Ook voor niet-vitale systemen, die formeel gezien buiten de IRB scope vallen, wordt eenzelfde aanbeveling gedaan.

Het vertragen van de (kerst)salarisbetalingen zorgt voor onrust op straat (rellen, proletarisch winkelen), waardoor de ME moet optreden. Ondertussen blijven diverse groepen hun verstorende werkzaamheden doorzetten. Gehackte dynamische routepanelen boven de snelwegen zorgen voor een verkeersinfarct. In de hele Randstad worden metro- en tramsystemen door hackers gesaboteerd. De onrust op straat is inmiddels zo hoog opgelopen dat de burgemeesters van de grote vier steden een noodverordening instellen die tot 28 december zal gelden om verdere plunderingen te voorkomen. De onrust zorgt er zelfs voor dat de Elfstedentocht, die met veel enthousiasme is aangekondigd, wordt afgeblazen omdat de politie niet kan garanderen dat men voldoende personeel kan leveren.

Nederland ligt duidelijk breed onder vuur van de ervaren internationaal opererende hackers van Ahackgroup. Andere minder professionele groepen en/of eenlingen haken aan, maar verliezen na een aantal dagen hun focus en gaan weer over tot de orde van de dag.

Na deze serie incidenten wordt door veel verschillende partijen gewerkt aan herstelmaatregelen. Ook oefent de Tweede Kamer achteraf via moties veel druk uit op de ministeries van Buitenlandse Zaken en van Veiligheid en Justitie om onverwijld te zorgen voor internationale wetgeving en verdragen voor de aanpak van eventueel volgende cyber aanvallen op Nederland. De Kamerleden dringen er op aan dat Buitenlandse Zaken de landen waarvandaan Nederland is aangevallen, onder druk zet om handelend op te treden. Deze landen geven echter aan niet direct iets te kunnen doen aangezien het allerminst zeker is dat de aanvallers ook daadwerkelijk uit hun land komen. Mogelijk zijn geïnfecteerde computers in hun land door aanvallers van elders misbruikt. Ook hebben niet alle landen een even goed functionerende overheidsCERT.
Een langdurige onrust en een gevoel van onveiligheid na een ernstige periode van zwaar hacktivisme zorgen ervoor dat berichtgeving over een nieuwe hack – of deze nu waar is of niet – snel kan leiden tot een paniekreactie of nieuwe sociale onrusten bij burgers en het MKB.

Impact en waarschijnlijkheid
Dit scenario wordt door de experts vanwege de combinatie van verschillende gebeurtenissen en de gebondenheid van het scenario aan een specifieke periode en

specifieke weersomstandigheden als minder waarschijnlijk geacht. De afzonderlijke gebeurtenissen worden daarentegen wel bijna allemaal als reëel gezien. Van de vitale belangen wordt geen enkele echt aangetast in het scenario, wel ondervinden ze hinder van de gebeurtenissen, net als de net niet als vitaal aangemerkte organisaties en functies. De impact van het scenario wordt door de experts als aanzienlijk tot ernstig gekwalificeerd. Die impact wordt bepaald door de gevolgen van de grotendeels ongecoördineerde acties van hacktivisten waarmee het functioneren van onder meer nutsvoorzieningen, industriële processen, betalingssystemen en informatiesystemen wordt verstoord. Doordat de acties plaatsvinden in een periode rond kerstmis, waarin het ook nog eens een tijd lang flink vriest, leidt de combinatie van sommige verstoringen tot uit de hand lopende situaties. Op diverse plaatsen ontstaan er rellen en plunderingen, het verkeer en openbaar vervoer ondervinden zware hinder, er doen zich vele (kleine en grotere) ongevallen voor en de met groot vertoon van enthousiasme aangekondigde Elfstedentocht wordt op het laatste moment afgelast. Dat alles veroorzaakt veel onrust, woede en een zekere mate van burgerlijke ongehoorzaamheid onder de bevolking. Er ontstaat een forse materiële schade en ook de economische schade voor het bedrijfsleven is groot. De internationale positie van Nederland lijdt schade door acties van buitenlandse hacktivisten, boycot van Nederlandse producten en terugval van het toerisme. Gedurende één tot twee dagen is het dagelijkse leven aanzienlijk verstoord en door de druk op de hulpdiensten kunnen er 'onnodig' enkele doden en tientallen zwaargewonden vallen.

Scenario Gewelddadige eenling
De afgelopen jaren is de samenleving meermalen geconfronteerd met eenlingen die geweld ter hand nemen. Soms maken deze personen deel uit van een (ideologisch) netwerk, wat aanknopingspunten biedt om gewelddadigheden te voorkomen. Terroristische netwerken worden immers geïdentificeerd en in de gaten gehouden. In dit scenario is gekozen voor een eenling die geen deel uitmaakt van een netwerk en geen verwarde psychiatrische patiënt is. Deze eenling pleegt solistisch een reeks aanslagen, waarbij niet direct duidelijk is in welke richting de dader moet worden gezocht. Het scenario speelt in een nabije toekomst waarin een context wordt geschetst door economische onzekerheid (hoge werkloosheid, gestegen rente en aanhoudende euro- en bankencrisis) en toegenomen wantrouwen: bestuurders, directeuren en politici worden in de media veelal omschreven als graaiers, waar eerlijke burgers het slachtoffer van zijn.

Een 42-jarige procestechnoloog verliest zijn baan bij een groot elektronicaconcern. Eerder al is hij in aanraking geweest met de bedrijfspsycholoog en deze constateert dat hij star gedrag vertoont wat hem onder meer parten speelt bij veranderingen in de organisatie. Niettemin heeft hij altijd goed gefunctioneerd en werd dit gedrag niet als belemmerend gezien. Na zijn ontslag raakt hij meer en meer geïsoleerd van zijn gezin. Hij vindt geen nieuwe baan en de schulden nemen toe. De hypotheekrente is fors gestegen en Nederlanders die hun huis moeten verkopen, blijven met een flinke restschuld zitten. Ook zijn huis wordt moeilijker verkoopbaar. Hij voelt zich steeds meer in het nauw gedreven, door oorzaken waar hij zelf geen grip op heeft. Hij verliest zich op zijn zolder in het op internet lezen over de financiële crisis en uitwassen rond bankiers, bestuurders en politici. Tegen zijn vrouw zegt hij druk met solliciteren bezig te zijn.

In de loop van een aantal maanden worden in het scenario drie aanslagen gepleegd met dodelijke afloop. Eerst wordt een directeur van een grote bank neergeschoten vlakbij zijn auto. Enkele maanden later ondergaat een hoge UWV bestuurder hetzelfde lot. Beide

moorden zijn zorgvuldig beraamd, koelbloedig en zonder achterlating van sporen gepleegd. Het volgende slachtoffer is een hoogleraar, tevens oud politicus en voormalig Europees commissaris, met uitgesproken ideeën over de heilzame werking van de markt, het streven naar eigenbelang en herinvoering van tucht. Deze man schrijft columns en treedt regelmatig op in praatprogramma's op televisie. Na de moord op hem worden er verbanden gelegd met de eerdere moorden en wordt het onderzoek geïntensiveerd.

In de media ontstaat grote aandacht voor de aanslagen. De angst neemt toe omdat de aanslagen niet worden opgeëist en onbekend is welke persoon of groepering er achter zit. Sommigen, vooral bestuurders, politici en captains of industry, voelen zich ongemakkelijker en mijden publieke optredens. Hiernaast zijn er groeperingen in de samenleving die de aanslagen als logisch gevolg van de kapitalistische uitwassen van de afgelopen jaren beschouwen en afgeven op het EU beleid, wat tot uiteenlopende reacties uit het buitenland leidt.

Enkele maanden later wordt voor het eerst weer concrete voortgang geboekt in het onderzoek. Men besluit uiteindelijk een compilatiefilmpje te maken met beelden van beveiligingscamera's. Alvorens de beelden op televisie uit te zenden zoeken de rechercheurs contact met de bedrijfspsycholoog van het elektronicaconcern, dat eerder in het onderzoek reeds naar voren was gekomen. De psycholoog geeft aan voordat hij kennis wil nemen van de beelden, eerst ruggespraak met zijn beroepsvereniging te willen hebben over dit in zijn ogen verregaande verzoek. De politie besluit hier niet op wachten; dezelfde avond worden de beelden, hoe vaag ook, vertoond in het programma Opsporing verzocht. De vrouw van de procestechnoloog herkent haar man en tipt de politie. De politie doorzoekt zijn huis. Hij is ondertussen zelf op de vlucht geslagen. In zijn zolderkamer wordt een lijst met mogelijke doelwitten aangetroffen, waaruit blijkt dat mogelijk een volgend slachtoffer onder politici moet worden gezocht. De druk en onrust nemen toe met ieder uur dat hij vrij rondloopt, in het bijzonder onder deze groep. Werkzaamheden van Kamerleden worden opgeschort, politici duiken onder. Enkele dagen later kan de man worden aangehouden.

Impact en waarschijnlijkheid
Een aantal maatschappelijke ontwikkelingen maakt dit scenario voorstelbaar. Er zijn economische omstandigheden die tot frustraties kunnen leiden. Het is mogelijk om in Nederland aan een wapen te komen. Personen met een profiel zoals beschreven in het scenario komen voor in onze samenleving, al zullen veruit de meesten niet overgaan tot dergelijke acties. Ook zijn de in het scenario beschreven acties van een 'onzichtbare eenling' moeilijk te voorkomen, omdat zulke personen zich buiten het zicht van de instanties bevinden. Daardoor wordt het scenario als waarschijnlijk beoordeeld.
De impact van de acties van de gewelddadige eenling worden niet als heel groot of ernstig ingeschat, voornamelijk omdat zijn slachtoffers deel uit maken van een specifieke doelgroep. De drie aanslagen met dodelijke afloop die de gewelddadige eenling pleegt zorgen wel voor grote aandacht in de media en toenemende angst en spanning in de samenleving. Dat komt vooral doordat het laatste slachtoffer een bekende oud-politicus is met een vrij uitgesproken mening. En omdat dan duidelijk wordt dat de dader, die nog vrij rond loopt, het heeft gemunt op onder meer bestuurders, politici, bankiers en captains of industry. Er zijn felle discussies over de vrijheid van meningsuiting en over de rol van 'het grote geld'. Die hebben – tijdelijk – een aanzienlijk effect op de democratische rechtstaat, maatschappelijke onrust en woede en de internationale positie

van Nederland. De overige impactcriteria scoren laag en de vitale sectoren en diensten worden niet aangetast.

Scenario Grootschalige onlusten

In het jaar 201X worden de Nederlandse maatschappelijke verhoudingen sterk bepaald door een grote onvrede onder een belangrijk gedeelte van de burgers (vooral jongeren) ten aanzien van gezaghebbende instituties zoals de politiek, openbaar bestuur, rechtspraak, onderwijs en gezondheidszorg. Ook al heeft dit `grote ongenoegen' nog niet geleid tot een actief verzet tegen deze instituties, er broeit wel degelijk iets.

In de zomer van 201X vinden in Amsterdam ineens een groot aantal flashrobs plaats. Een groep jongeren die elkaar veelal niet kennen spreekt via sociale media af op een bepaalde locatie om op hetzelfde moment een winkel te overvallen of mensen op straat te beroven. De aandacht voor de flashrobs in de media zorgt voor toenemende onrust onder inwoners van Amsterdam. Kunnen ze nog wel veilig de straat op? De hype van de flashrobs slaat al snel over naar andere steden in de Randstad. Winkeliersverenigingen in de steden zetten massaal private beveiligingsbedrijven in om hun winkels te beveiligen tegen de criminele jongeren. Steeds vaker wordt er ook geweld gebruikt, worden vernielingen aangericht en worden winkels geplunderd. De flashrobs worden door andere groepen, zoals anarcho-extremisten, aangegrepen om hun ideologieën meer kracht bij te zetten. De politie heeft ondertussen de grootste moeite om iets te doen tegen het geweld in de steden, wat direct zorgt voor problemen met de lokaal beschikbare politiecapaciteit. Ondertussen ontstaat ook op de betrokken departementen grote bezorgdheid over de onrust in de Randstad.

De vlam slaat echter in de pan wanneer het eerste dodelijke slachtoffer valt bij een gewelddadige flashrob. Via sociale media worden burgers opgeroepen om in actie te komen tegen het falen van de politie en het bestuur om iets te doen tegen het geweld op straat. Dit leidt ertoe dat honderden mensen in Amsterdam, Rotterdam en Den Haag de straat op gaan met de eis aan bestuurders om in te grijpen. En dat winkeliers en burgers buurtwachten organiseren om wijken te beschermen tegen criminele jongeren. Verschillende politici roeren zich en vragen om een spoeddebat in de Tweede Kamer. Als er een tweede slachtoffer valt escaleert de situatie volledig. Een Marokkaans-Nederlandse jongen, die onterecht wordt aangezien als plunderaar overlijdt na een vechtpartij met een buurtwacht. Als reactie op de dood van de jongen bestormt een grote groep jongeren, gemobiliseerd via de sociale media, een politiebureau en vinden grootschalige rellen plaats.

De dag daarop blijven er, ondanks scherpe veiligheidsmaatregelen, in verschillende grote steden gewelddadige plunderingen plaatsvinden. Via sociale media wordt als reactie hierop telkens opgeroepen tot demonstraties tegen deze plunderingen. De ME voert verschillende charges uit om betogers en tegenbetogers uit elkaar te houden. Op sociale media verschijnen opruiende berichten en wordt er volop gespeculeerd over het wie, wat en waarom van het geweld. De situatie wordt in de steden snel onoverzichtelijk en op meerdere plekken in het land vinden rellen plaats. Zowel de politie als de hulpverleningsdiensten kampen inmiddels met capaciteitsproblemen.

Vanuit de landelijke overheid wordt getracht meer regie te krijgen op de aanpak van de onlusten in het land. Zo wordt de overheidscommunicatie rondom de gebeurtenissen te versterkt door onder meer de inzet van sociale media om de burgers zo adequaat

mogelijk te informeren zonder onrust te zaaien. Het is echter moeilijk om grip te krijgen op alle lokale initiatieven van communicatie met de burgers en de pers. Ook op andere vlakken loopt de afstemming tussen landelijke en lokale overheid over de aanpak van de onlusten in het land alles behalve soepel. Het voornemen van de de minister van V&J om politie-eenheden uit heel het land opdracht te geven tot bijstandsverlening aan de politie in de vier grote steden leidt tot een hoogoplopende ruzie tussen het nationale en lokale gezag.

De onlusten vinden inmiddels niet meer alleen plaats op straat maar ook op internet. Diverse overheidswebsites hebben te kampen met digitale aanvallen. Ook wordt het Twitteraccount van het NCC gehackt door anarchisten, die vervolgens desinformatie verspreiden.

De volgende dagen breiden de onlusten zich snel verder uit over het gehele land. De situatie in de steden wordt uiterst chaotisch met massale rellen, plunderingen en brandstichtingen. In centra van grote steden heerst een oorlogssfeer, met winkels die gesloten zijn en ramen die zijn dichtgetimmerd na de plunderingen. Ouders houden hun kinderen thuis vanwege de onrust op straat. Door de chaos in de straten rijden bussen en trams niet en is het onmogelijk geworden om met de auto het stadscentrum te bereiken. Bedrijven en winkels in de stadscentra sluiten hun deuren, enkel beveiligd door private bewakingsdiensten. Brandweerinzet en geneeskundige hulpverlening worden in de grote steden alsmaar moeilijker. Het personeel kan in een aantal wijken slechts opereren met de hulp van ME-ers. De politie heeft in elke politieregio de handen vol om de situatie te proberen te beheersen, waardoor aan verzoeken om bijstand in andere regio's niet kan worden voldaan. De capaciteit van de politie is uitgeput. De KMAR wordt ingezet om ondersteuning te bieden aan de politie, maar ook die extra capaciteit dreigt snel uitgeput te raken. Op overheidsniveau wordt meer en meer gedacht aan een verdere inzet van andere militaire overheden. Ook wordt buitenlandse hulp ingeroepen. Zo wordt de politie in de grensregio's bijgestaan door collega's uit Belgie en Duitsland.

De lokale overheden worden aangespoord om sleutelfiguren van wijken en gemeenschappen te mobiliseren om in eigen kring dempend te werken. Er wordt getracht om via (sociale) media een 'vreedzame tegenbeweging' te organiseren. Op verschillende plekken in het land ontstaan spontane burgerinitiatieven, bijvoorbeeld om de straten schoon te vegen na plundering of om voedsel te brengen naar mensen die de straat niet meer op durven. Als de grootschalige onlusten uiteindelijk ten einde zijn gekomen, wordt stevig ingezet op opsporing van de plunderaars die met snelrecht direct voor de rechter worden gebracht en veroordeeld. Uiteindelijk keert de rust in het land terug. De naweeën van de chaos werken echter nog jarenlang door.

Impact en waarschijnlijkheid
De beschreven gebeurtenissen leiden tot veel maatschappelijke onrust, een forse aantasting van onze rechtstaat en de kernwaarden van onze samenleving en een aanzienlijke verstoring van het dagelijkse leven. De ontstane materiële en economische schade en ook de bestrijdingskosten zijn groot. Ons land loopt internationaal gezien 'imagoschade' op en toeristen zullen Nederland enige tijd mijden. Er vallen enkele doden en een flink aantal gewonden. Bij elkaar leidt dit tot een totale impactscore zeer ernstig. De kans dat dit extreme scenario zich binnen enkele jaren in Nederland gaat voltrekken wordt geschat op enigszins waarschijnlijk, mede gezien de nog steeds voldoende mate van weerstand en weerbaarheid bij overheid en samenleving. Wat betreft de

kwetsbaarheid van onze maatschappij ten aanzien van de gebeurtenissen in dit scenario wezen experts op de momenteel nog goed functionerende thermometerfunctie die lokale overheden bij specifieke bevolkingsgroepen hebben. Daar staat tegenover dat de overheid momenteel een achterstand heeft op het gebied van sociale media, hoewel er diverse initiatieven in de steigers staan om deze achterstand op te heffen.

Scenario Internationaal – Wapenbeheersing falende staat

Dit scenario speelt zich af in een fictief, niet-Europees land met een centrale democratische overheid maar een, historisch gezien, onzekere stabiliteit. Zowel het leger als het politieke systeem worden gekenmerkt door seculiere elementen maar in grotere mate ook door de politieke islam. In het land leven meerdere bevolkingsgroepen die onderling verschillen in etniciteit en religie, maar de grote meerderheid is moslim. De regio waarin het land ligt wordt gekenmerkt door regelmatig optredende grensconflicten en een gespannen geopolitieke situatie. Verslechterende omstandigheden en groeiende onvrede over de zwakke en door corruptie getroffen overheid en het falen van cruciale diensten, zoals de rechtspraak, onderwijs en gezondheidszorg zorgen voor toenemende instabiliteit. Tegelijkertijd neemt de opkomst van islamistische radicalisering in de samenleving, die een paar jaar eerder begonnen is, in kracht toe. Het land glijdt af naar een 'falende staat'. Na de verkiezingen in het jaar 201X behaalt geen enkele partij een duidelijke meerderheid. Na maanden van politiek gekibbel besluit het leger in te grijpen en wordt eind 201X een tijdelijke militaire regering aangekondigd. De verdeeldheid tussen groeperingen in het land blijft echter geleidelijk aan toenemen.

In mei 201X+2 blijkt uit inlichtingen dat mogelijk door een inside-job een onbekend aantal kernkoppen en een onbekende hoeveelheid plutonium afkomstig uit een verrijkingsinstallatie zijn zoekgeraakt. Een dag later laten drie generaals in een videoboodschap via nationale media en YouTube weten dat zij in het belang van het land en het geloof controle hebben genomen over een aantal nucleaire wapens. Zij dreigen desnoods deze middelen in te zetten.
Op de Nederlandse televisie en in de internationale media nuanceren experts direct de dreiging. Het lijkt zeer onwaarschijnlijk dat diegenen die de kernkoppen in handen hebben ook daadwerkelijk de middelen hebben om ze tot ontploffing te brengen. In ieder geval hebben ze geen raketsysteem waarmee Europa of de Verenigde Staten kan worden bereikt. Door deze geruststellende woorden blijft het publiek rustig onder de gebeurtenissen.
In de regio waarin de falende staat ligt, lopen de spanningen tussen landen op. Binnen de NAVO en in de VN Veiligheidsraad ontstaan hevige discussies over uitbreiding van de militaire aanwezigheid in de regio. Deze discussies worden bemoeilijkt door meningsverschillen over de status van de regering van de falende staat.

In juli 201X+2 wordt in Almere een groep mannen aangehouden die wordt verdacht van het plannen van terreurdaden. In een actualiteitenprogramma wordt deze Almeregroep afgeschilderd als nucleaire terroristen. Ondertussen gaat het diplomatieke getouwtrek over de situatie in de falende staat door. Nog steeds is het totale aantal missende kernkoppen niet duidelijk, maar inlichtingen gaan er vanuit dat het gaat om een vijftal van 12 kiloton.
Niet veel later wordt één van de kernkoppen ontdekt in een grote havenstad in een niet-westers land. Een week later verschijnt een nieuwe videoboodschap waarin de radicalen dreigen met een nucleair conflict als de Westerse landen zich niet uit de regio terugtrekken.

Op 16 oktober 201X+2 wordt in de haven van Rotterdam een nucleaire lading ontdekt in een container uit een havenstad buiten Europa. Het blijkt een van de vermiste kernkoppen te zijn.
Direct na de ontdekking wordt in alle stilte een deel van de haven afgesloten en worden alle crisismechanismen in werking gezet. Nationale overheden, ook van omringende landen, nemen maatregelen zoals scherpere controles bij mainports. Enkele uren na de ontdekking in Rotterdam hebben media lucht gekregen van de gebeurtenissen. Zij wekken de indruk van een grootschalig terreuroffensief dat doet denken aan een nucleair 9/11. Hoewel de officiële woordvoerders met een eenduidig beeld naar buiten treden, vertellen verschillende experts in de media tegenstrijdige verhalen. Burgers weten niet precies wie gelijk heeft en gaan van het ergste uit. De 'zogenaamde kenners' hadden immers enkele dagen daarvoor nog verkondigd dat de missende kernkoppen nooit een bedreiging voor Europa kunnen vormen, maar nu ligt er één in de Rotterdamse haven. In de paniek die ontstaat wordt worden op last van bezorgde burgemeesters ook andere havens in Nederland gesloten.
In de loop van 16 oktober wordt duidelijk dat de kernkoppen technisch niet tot ontploffing kunnen worden gebracht en dus geen directe dreiging vormen. De verschillende Nederlandse havens worden na één tot twee dagen weer volledig vrijgegeven. De berichtgeving in verschillende media blijft echter onrustig. Tevens is het publiek niet bekend met dit type dreiging, wat de onzekerheid, angst en onrust vergroot.

De gebeurtenissen doen ook het debat over moslims en integratie opnieuw oplaaien. De tolerantie ten aanzien van de moslimbevolking in Nederland vermindert en in de media van moslimlanden wordt zeer kritisch gesproken over de hegemonistische houding van het Westen. De falende staat wordt een safe haven voor mondiaal Jihadisme. Fatwa's tegen het Westen en "onwaardige regeringen" in de regio krijgen toenemend gehoord onder jonge mensen. Ook vanuit het Westen, waaronder Nederland, reizen personen af om zich aan te sluiten bij de mondiale strijd. De dreiging van nucleair terrorisme en een mogelijk kostbare interventie in de regio waar de falende staat ligt zorgen voor onzekerheid en negativiteit op de internationale markten. Consumenten- en producentenvertrouwen in Nederland zakken fors. De wereldeconomie die juist er bovenop leek te krabbelen krijgt weer een flinke klap.

Impact en waarschijnlijkheid
Het totale scenario wordt onwaarschijnlijk tot enigszins waarschijnlijk geacht. De beschreven destabilisering in 'de falende staat' en ontvreemding van kernwapens door een 'inside job' worden niet voor onmogelijk gehouden. Dat één van de kernkoppen nu net in Nederland wordt ontdekt is echter toeval. De onrust door de nucleaire dreiging en de toenemende polarisatie in de samenleving worden zeker voorstelbaar geacht.
De impact van de gebeurtenissen wordt als zeer ernstig ingeschat. Vooral de aantasting van de integriteit van de internationale positie van Nederland en de aantasting van de democratische rechtstaat spelen hierbij een grote rol. De onrust onder de bevolking als gevolg van de nucleaire dreiging zorgt daarnaast voor een hoge sociaal-psychologische impact.

3 Agenderingsadvies capaciteiten

3.1 Inleiding

In hoofdstuk 2 is aandacht besteed aan de NRB 2012. De resultaten van de NRB zijn vervolgens gebruikt voor het uitvoeren van de capaciteitenanalyse. Tijdens deze analyse is met een groot aantal experts in kaart gebracht welke capaciteiten[6] wij (overheid, bedrijfsleven en burger), uitgaande van de capaciteiten die we nu reeds hebben, zouden moeten versterken om de risico's en dreigingen zoals beschreven in de NRB beter te kunnen hanteren. Zie bijlage 1 voor de samenvatting van de uitkomsten van deze 'capaciteitenanalyses'.

Op basis van door de deskundigen geadviseerde capaciteiten is in overleg tussen de verantwoordelijke ministeries een selectie gemaakt. Hierbij is gelet op onder meer doelmatigheid en toegevoegde waarde in vergelijking met eerder vastgestelde capaciteiten. Verder is vooral gezocht naar capaciteiten die breed inzetbaar zijn zodat een investering maximaal effect heeft en is waar mogelijk rekening gehouden met hetgeen momenteel gebeurt en ontwikkeld wordt. De geselecteerde capaciteiten zijn tenslotte samengevat in een capaciteitsadvies. De scenario's uit de NRB 2012 bevestigen voor een deel trajecten die al lopen; de te versterken capaciteiten betekenen derhalve een intensivering van die trajecten.

Het kabinet beslist op basis van de bevindingenrapportage welke aanbevelingen worden uitgevoerd. In dit hoofdstuk worden de geselecteerde capaciteiten en het capaciteitsadvies beschreven.

3.2 Aanbevelingen 2012

De te versterken capaciteiten, zoals die uit de verschillende capaciteitenanalyses naar voren komen, zijn onderverdeeld in vijf thema's:

1. samenwerking bij crisisbeheersing
2. informatiepositie
3. bewustwording en scholing
4. crisiscommunicatie
5. internationaal te agenderen capaciteiten

Binnen deze generieke thema's wordt geadviseerd een aantal specifieke capaciteiten op te pakken. In de volgende paragrafen worden deze nader toegelicht.

---

[6] Een capaciteit is het vermogen van de (rijks)overheid, private partners en burgers om taken uit te voeren die (mede) tot doel hebben de nationale veiligheid te beschermen. Het gaat hierbij om bepaalde combinaties van middelen (bijv. materiaal of informatiesystemen), mensen (civiel, militair, et cetera) en methoden (zoals procedures, plannen, oefenen, publiek-private samenwerkingsverbanden).
Capaciteiten helpen de kans en/of de impact van een of meerdere dreigingen te reduceren.

3.2.1 Samenwerking bij crisisbeheersing

Inleiding
Een goed op elkaar afgestemde en op elkaar ingespeelde crisisorganisatie is cruciaal voor een tijdige en adequate respons. In eerdere bevindingenrapportages zijn op dit terrein adviezen uitgebracht. Daarbij is vooral aandacht geweest voor generieke processen, zoals bijvoorbeeld het instellen van de Landelijke Operationele Staf (LOS) en het vergroten van de slagvaardigheid van besluitvorming bij crises. De beoordelingen van de scenario's over cyberhacktivisme, grootschalige onlusten en internationale vraagstukken geven aan dat het voor deze onderwerpen nodig is om nog specifiek de samenwerking bij crisisbeheersing op een aantal punten te versterken.

(inter)nationale samenwerking cybercrisis
Het idee dat een ICT verstoring kan leiden tot een crisis op nationaal en zelfs internationaal niveau is een vrij nieuw thema in de wereld van crisisbeheersing. Er is voor dit type crisis inmiddels een aantal maatregelen genomen, maar toch zijn hier nog versterkingen aan te brengen. Aangezien een cybercrisis vaak ook een internationale dimensie heeft, dient doorlopend geïnvesteerd te worden in de versterking van de internationale samenwerking. Daarnaast is een verdere ontwikkeling van de capaciteiten van de nationale partners, met name in de veiligheidsketen (zowel naar andere overheden als private partners) nodig. Het doel is dat de aanpak van ICT crisisbeheersing een volwaardig onderdeel is van de nationale crisisstructuur in Nederland waarin alle betrokken partijen hun rol en verantwoordelijkheid kennen. Het Nationaal Cyber Security Centrum (NCSC) vervult hierin een coördinerende rol.
Concreet worden hiertoe een aantal acties voorgesteld:

- Opstellen van samenwerkingsafspraken over ondermeer informatie-uitwisseling tijdens een crisis met NCSC en medeoverheden en vitale private partners ten tijde van crisis. Producten: Nieuwe versie Nationaal Crisisplan-ICT (gereed: eerste helft 2014) en samenwerkingsafspraken met partners. (continue bezigheid gezien het groot aantal publieke en private partners)
- Preparatie op cyberincidenten en –crises door middel van het beoefenen van de nationale samenwerking tussen ketenpartners. Product: nationale oefeningen. (continue activiteit, eerstvolgende nat. oefening in tweede helft 2014)
- Verbeteren van de internationale samenwerking door middel van een inventarisatie van de verschillende aanpakken van cyber security en de responscapaciteiten. Product: internationale benchmark methoden van aanpak. (gereed: medio 2014)
- Bestaande internationale afspraken en samenwerkingsmethoden (IWWN Standard OP en EU SOP) bekrachtigen en toepassen. Producten: Actuele SOP's en internationale oefeningen. (continue bezigheid, int. oefeningen vinden tweejaarlijks plaats)

Wie is verantwoordelijk: *Minister van Veiligheid en Justitie* als coördinerend minister voor cyber security.

Samenwerking op terrein van bijstand
In de voorbereiding op de respons op grootschalige onlusten wordt al een Nationaal Crisisplan Rellen ontwikkeld, dat de interdepartementale crisisstructuur specificeert bij grootschalige rellen. In aanvulling hierop wordt geadviseerd om de mogelijkheden van

samenwerking met andere partners uit te werken. De dagelijkse taakuitvoering van de politie op straat is binnen dit extreme en uitzonderlijke scenario van onlusten die om 24/7 inzet vragen, zonder andere inzet of bijstand, beperkt en kan binnen enkele dagen uitgeput raken. Hiertoe dienen de mogelijkheden van en voorwaarden voor samenwerking met andere partners te worden uitgewerkt en in afspraken vastgelegd (op hoofdlijnen). Hierbij valt te denken aan de inzet van defensie-eenheden en publiek-private partnerschappen. Daarbij is het belangrijk om een real time (kwalitatief en kwantitatief) overzicht te creëren van de beschikbare bijstandscapaciteit (en de kosten daarvan).
Op grond van de Politiewet 2012 en in het kader van civiel-militaire samenwerking kan al ten behoeve van handhaving van de rechtsorde bijstand van Defensie worden gevraagd. De in de capaciteitenanalyse geprioriteerde capaciteit gaat over het voortzettings-vermogen bij uitputting van politiecapaciteiten. Hierbij valt bijvoorbeeld te denken aan het laten uitvoeren van backoffice taken van de politie door defensiecapaciteit en het front naar de burger 'blauw' te houden.
Wie is verantwoordelijk: *Minister van Veiligheid en Justitie*

Aansluiting plannen nucleaire dreiging
In het geval van een internationale nucleaire dreiging bestaat er geen compleet beeld over hoe internationale, nationale en regionale (inclusief lokale) plannen op elkaar aansluiten. Dit moet nader onderzocht worden. Duidelijk moet worden welke organisaties en structuren (inclusief hun bijbehorende plannen) een betrokkenheid en bevoegdheid hebben bij een dergelijke dreiging. Te beantwoorden vragen o.a. waar zitten hiaten? Hoe sluiten structuren en processen op elkaar aan? Wat is de koppeling van de generieke crisisstructuur, NPK, ATb, NAVO, bestaande procedures? Een dergelijke analyse moet de taakverdeling zowel nationaal als internationaal verduidelijken en moet voldoende basis bieden voor een inventarisatie van afspraken over de inzet van internationale response units binnen de context van de NAVO, EU. Tevens biedt het de basis van het stroomlijnen van de betrokken plannen.
Wie is verantwoordelijk: *Minister van Veiligheid en Justitie, de minister van Economische Zaken en de minister van Buitenlandse Zaken*.

3.2.2 Informatiepositie

Inleiding
Uit de beoordeling van de scenario's Cyberhacktivisme, Grootschalige Onlusten en Internationaal blijkt dat een verbeterde informatiepositie van de overheid een belangrijke capaciteit is bij het verminderen van de waarschijnlijkheid dat dergelijke incidenten zich voordoen.

Detectie- en analysecapaciteit
ICT aanvallen en verstoringen zijn lang niet altijd direct zichtbaar. Er kan bijvoorbeeld al malware actief zijn, voordat daadwerkelijk een verstoring of uitval optreedt. Om de kans op incidenten te verkleinen is het belangrijk dat deze malware tijdig gedetecteerd wordt. Het in kaart brengen en volgen van digitale dreigingen is nodig om een situational awareness te hebben, trends waar te nemen en om tijdens incidenten en crisissituaties snel een goede duiding te kunnen geven. De cyberdetectie en analysecapaciteit is ook benodigd voor het kunnen leggen van verbanden tussen ogenschijnlijk losstaande

incidenten en ontwikkelingen. De analyse capaciteit vereist specialistische systemen en personeel. Omdat de ICT wereld steeds verder groeit, en het cybersecurity veld onderhevig is aan snelle ontwikkelingen is het van belang dat ook een dergelijke analyse capaciteit zich continu verder operationeel ontwikkelt en dat mogelijkheden voor vroegtijdige detectie van malware en aanvallen steeds verder verbetert. Een eerste vereiste hierbij is het uitbreiden van de technische infrastructuur en personele capaciteit en kwaliteit.
Detectie is een eerste en uiterst belangrijke stap, maar de informatie die hieruit naar voren komt, verdient een snelle en grondige analyse ten behoeve van duiding en het bieden van handelingsperspectief. Daarnaast dienen ook andere informatiebronnen aangeboord te worden (zoals sociale media bronnen) om actuele ontwikkelingen te kunnen volgen en duiden. Tevens biedt de informatie uit onder andere de structurele detectieactiviteiten de gelegenheid om risico's voor de langere termijn te onderkennen. Dit vergt een ander type analyse en duiding dan die in het kader van de korte termijn respons activiteiten. Daarnaast kunnen gebreken in detectiecapaciteit door goede analyse aan het licht komen, en kan analyse leiden tot nieuwe inzichten om detectie te verbeteren. Er wordt dan ook geadviseerd om de analysecapaciteit uit te breiden, zodat er meer ruimte komt voor real time identificatie en duiding van incidenten, er meer zicht komt op nieuwe dreigingen en ontwikkelingen via sociale media analyse, malware analyse en het in kaart brengen en volgen van malafide infrastructuren zoals botnets. Van belang is hierbij ook dat er ruimte komt om lange termijn risico's te onderkennen .
Waar het gaat om *moedwillige* verstoringen is het ook zaak om voldoende capaciteiten te hebben om te kunnen opsporen en vervolgen.
Wie is verantwoordelijk: *Minister van Veiligheid en Justitie, Minister van BZK, Minister van Defensie.*

Informatiepositie mbt grootschalige onlusten
Om beter zicht te krijgen op voedingsbodems voor onrust maar ook op verstoorders van de openbare orde (bijv. de nieuwe hooligans), is het nodig de informatiepositie en ook opsporingsmogelijkheden van de overheid te verbeteren. Daarnaast dient de analysecapaciteit te worden versterkt om de complexe informatie uit verschillende bronnen te kunnen duiden.
Bovendien zou meer aandacht moeten komen voor monitoring en analyse van sociale media. Het gaat hierbij om het ontwikkelen/versterken van de kennis, vaardigheden en voorzieningen om sociale media (twitter, facebook etc) doelmatig te monitoren en te analyseren (zoals ook wordt geadviseerd ten behoeve van cyber). Versterking vraagt om het aanschaffen en ontwikkelen van software, maar ook en vooral om het ontwikkelen van competenties van personeel. Dit sluit aan bij het advies uit het rapport "Twee werelden: hoofdrapport commissie 'Project X' Haren"[7] om sociale media als een vast onderdeel van het dagelijks leven te monitoren, waarbij het gaat om het vinden van collectieve patronen die opmerkelijk zijn en mogelijk actie vereisen.
Tijdens grootschalige onrust is er behoefte aan een integraal beeld van wat er in de samenleving leeft. Momenteel worden bepaalde trends gemist vanwege de versnippering van informatie uit verschillende rapportages. Hiertoe zou een analyse-instrument (gesloten box-principe) moeten worden ontwikkeld dat informatie over korte en lange termijn risico's samenbrengt met trends uit bestaande rapportages.
Wie is verantwoordelijk: *Minister van VenJ, Minister van BZK, politie, OM*

[7] Bijlage bij Kamerstuk 33571 nr. 1. Rapport is opgesteld nav de rellen in de gemeente Haren (Project X) op 21 september 2012.

Internationale informatiepositie inlichtingendiensten
Om een internationale dreiging vroegtijdig te kunnen onderkennen en af te wenden buiten Nederlands grondgebied is het nodig dat de diensten een eigenstandige informatiepositie hebben en aan bronverificatie kunnen doen. Hiertoe wordt geadviseerd om de beschikbare middelen en capaciteiten van de inlichtingen- en veiligheidsdiensten op efficiënte en effectieve wijze in te zetten. Voor de ambassadeposten is hierbij primair een taak weggelegd; de informatie van de inlichtingen- en veiligheidsdiensten is hieraan complementair. Een verbeterde informatiepositie vergroot de kans op signalering en het voorkomen van een dergelijk scenario. Vroegtijdige signalering in het buitenland draagt ook positief bij aan de mogelijke respons, bijvoorbeeld de mogelijkheid om gevaren te kunnen onderscheppen.
Wie is verantwoordelijk: *Minister van BZK, Minister van Defensie, minister van BZ (postennetwerk).*

3.2.3 Bewustwording en scholing

Inleiding
Om de kans te verkleinen dat bepaalde incidenten zich voordoen en om de weerbaarheid te vergroten, is het van belang om zowel bij burgers als bij professionals de bewustwording en de kennis verder te ontwikkelen. Dit geldt zowel op het gebied van digitale veiligheid als op de signalering van een mogelijk gewelddadige eenling.

Versterken van awareness door voorlichting en bewustwording digitale kwetsbaarheden
Gerichte voorlichting over allerlei vormen van digitale onveiligheid kan bijdragen aan de weerbaarheid van gebruikers. Zowel door de overheid als door het bedrijfsleven wordt met enige regelmaat via de verschillende media aandacht aan het onderwerp besteed. Enkele voorbeelden uit verleden en heden zijn: de campagne Surf op Safe, 3 keer kloppen, phishing campagne, wachtwoordencampagne, de eerste Alert Online campagne in 2012. Voorlichting is het meest effectief als deze gericht is op actuele thema's en op het bieden van handelingsperspectief voor specifieke doelgroepen. En goed voorbeeld hiervan is de website 'Bescherm je Bedrijf'. Deze door het programma Digibewust en Nederland ICT ontwikkelde website is eind 2012 volledig herzien zodat bedrijven uit het MKB en ZZP-ers hun beveiligingsbeleid op gebied van ICT kunnen toetsen. Een goede samenwerking tussen overheid en bedrijfsleven is hierbij cruciaal. Een ander voorbeeld is de (begin 2013) door de minister van BZK in het leven geroepen Taskforce Bestuur en Informatieveiligheid Dienstverlening. Doel van de Taskforce is enerzijds om samen met de koepelorganisaties binnen de overheid versnelling te weeg te brengen op het vlak van bewustzijn, anderzijds het ontwikkelen van concrete middelen om sturing op informatieveiligheid door bestuur en topmanagement binnen de overheidslagen mogelijk te maken. Het doel is om na twee jaar te komen tot verplichtende zelfregulering per overheidslaag.
Met de voortzetting van de campagne Alert Online wordt nu meer structureel dan in het verleden gebeurde, gewerkt aan voorlichting en bewustwording. Deze campagne sluit aan op de Europese acties die in dit kader elk jaar in de maand oktober worden georganiseerd.

Wie is verantwoordelijk: *De minister van Veiligheid en Justitie* als trekkers, in samenwerking met alle ministeries, private partijen, branche-organisaties en belangengroepen.

Scholingsprogramma's om kennis en kunde op gebied van cyber security te vergroten
In de Nationale Cyber Security Strategie (NCSS) is dit onderwerp als een van de actielijnen benoemd. Deze capaciteit heeft betrekking op het verbeteren van de professionaliteit van de ICT-beroepsbevolking op dit terrein. Doel is het stimuleren en ondersteunen van het opstellen en uitvoeren van een integraal scholingsprogramma waar verschillende ideeën en initiatieven bij elkaar gebracht moeten worden. Gestart moet worden met het inventariseren van de verschillende huidige programma's, acties en behoeftes (gereed: eerste helft 2014).
Wie is verantwoordelijk: *de minister van Veiligheid en Justitie voor inventarisatie als coördinerend minister voor cyber security*

Kennis op gebied van potentieel gewelddadige eenlingen

Om het risico dat uit kan gaan van gewelddadige eenlingen zoveel mogelijk te beperken, moeten kennis en handelingsperspectieven onder eerstelijnsprofessionals en de mogelijkheden tot het delen van kennis en expertise worden uitgebreid.

Hiertoe is een drietal prioriteiten benoemd:

1. Het oprichten van een 'Operationeel advies- en expertisepunt', op regionaal of landelijk niveau. Dit richt zich op het delen van kennis en expertise op casusniveau, voor en tussen professionals uit zorg, welzijn, geestelijke gezondheidszorg, politie, reclassering, OM, etc. Dit gebeurt vanzelfsprekend met inachtneming van de privacybescherming. Het punt is bedoeld als platform waar eerstelijns professionals terechtkunnen voor praktische kennis, advies en doorverwijzing als zij casusgerichte vragen hebben over een (potentieel) gewelddadige eenling. Het is nadrukkelijk *geen meldpunt.* De verantwoordelijkheid met betrekking tot de casus/cliënt blijft bij de behandelende professional.

2. Het oprichten van een 'Centraal kennispunt'. Dit richt zich op het bundelen en beschikbaar maken van bestaande kennis en het verwerven van nieuwe kennis op het gebied van onderzoek, beleid, wetgeving en internationale ontwikkelingen. Het is belangrijk dat de twee informatiepunten (prioriteit 1 en 2), ondanks hun verschillende doelstellingen, goed met elkaar gekoppeld worden. Zij voeden en bevragen elkaar onderling en zorgen voor een duidelijke verbinding tussen de behoeften op regionaal en landelijk niveau.

3. Het bevorderen van specifieke vaardigheden onder professionals. Hiervoor zullen sommige basisopleidingen voor professionals versterkt en uitgebreid moeten worden zodat deze professionals meer inzicht zullen krijgen wat vroegtijdige signalering mogelijk maakt. Voor sommige beroepsgroepen bestaan dergelijke opleidingen/trainingen al. Onderzocht moet worden of deze opleidingen/trainingen beschikbaar gesteld moeten worden voor alle hulpverleners.

Met het oog op efficiency, wordt gestreefd naar ophanging van de beide punten binnen bestaande netwerken/structuren. Dit bespaart eventuele extra inzet van mensen en middelen. Waar noodzakelijk wordt aanvullende expertise ingehuurd.
Voor het totstandbrengen van deze drie prioriteiten zijn de ministeries van Veiligheid en Justitie, Binnenlandse Zaken en Koninkrijksrelaties en Volksgezondheid, Welzijn en Sport

gezamenlijk verantwoordelijk. Met betrekking tot het beperken van het risico dat uit kan gaan van gewelddadige eenlingen spelen namelijk zowel veiligheidsbeleid, inlichtingenwerk en de (geestelijke) gezondheidszorg een rol. Als het gaat om potentieel gewelddadige eenlingen beïnvloeden en versterken deze terreinen elkaar.

Trainingen en opleidingen op het terrein van crisisbeheersing voor diplomaten op posten.
De crisisbeheersing op het ministerie van Buitenlandse Zaken wordt steeds strakker geleid, maar posten weten te weinig over hoe op te treden tijdens crises. Op dit moment wordt een trainingsmodule ontworpen over hoe te handelen in crisistijd. De module wordt eerst uitgerold op hoog risico posten daarna naar andere.
Wie is verantwoordelijk: *de minister van BZ*.

3.2.4 Crisiscommunicatie

Communicatie is (naast bestuurlijke en operationele inzet) een van de drie pijlers in het vormgeven van een adequate crisisrespons. De afgelopen jaren is er al veel gedaan om crisiscommunicatie op een hoger niveau te krijgen, waardoor het zich tot een volwaardige discipline heeft ontwikkeld. De beoordeling van het cyberhacktivisme scenario, het scenario over grootschalige onlusten en het internationale scenario laten zien dat toevoeging van specifieke kennis van toegevoegde waarde is bij de communicatie over deze crisistypen

Zo wordt geadviseerd om de volgende twee onderwerpen specifieke aandacht te geven binnen bestaande nationale communicatieplannen of in bestaande crisisplannen met aandacht voor communicatie:

- ICT-crisis / hacktivisme
- Internationale moedwillige nucleaire dreiging

Daarnaast wordt geadviseerd om met betrekking tot grootschalige onlusten de nationale kaders voor crisiscommunicatie te verhelderen, zodat eenduidig kan worden gecommuniceerd naar de bevolking, maar met behoud van lokaal maatwerk. Eenduidige, effectieve crisiscommunicatie is één van de belangrijkste instrumenten bij het de-escaleren van maatschappelijke onrust.

In een tijd waarin steeds meer gebruik wordt gemaakt van sociale media als communicatiemiddel is het raadzaam dat ook de overheid, naast het monitoren van sociale media, deze communicatievorm meer gaat benutten als instrument om actief te communiceren bij crisis.

Naast sociale media spelen ook experts van buiten de overheid een belangrijke rol in de communicatie ten tijde van een (dreigende) crisis. Naar aanleiding van het internationale scenario wordt geadviseerd om het netwerk van experts met sociaal draagvlak in kaart te brengen en de relatie met dit netwerk met name in koude tijd te versterken. De relevante experts moeten in de koude fase proactief op de hoogte van overheidsmaatregelen en de overwegingen daarachter gehouden worden, zowel op inhoud als op organisatie (van bijvoorbeeld de rijkscrisisstructuur). Zo wordt getracht om een beter begrip te krijgen voor overheidsoptreden ten tijde van een crisis. Tegenstrijdige berichtgeving is dan beter te voorkomen.

Ten slotte zou de Nederlandse overheid bij crises met een internationale component rekening moeten houden met de effecten van maatregelen en communicatie op de internationale gemeenschap.
Wie is verantwoordelijk: *de minister van Veiligheid en Justitie.*

3.2.5 Internationaal te agenderen capaciteiten

Inleiding
Voor een tweetal capaciteiten geldt dat zij van dusdanige aard en omvang zijn, dat zij niet alleen binnen Nederland kunnen worden opgepakt. Nederland zal hier in internationaal verband steun voor moeten vinden en het onderwerp agenderen. Dit betekent ook dat voor het verbeteren van deze capaciteiten meer tijd benodigd is.

Basisrichtlijnen beveiliging bij ontwikkeling van hard- en software ('bouwbesluit cyber')
De weerbaarheid van de samenleving tegen de verschillende kwetsbaarheden bij de vele toepassingen van ICT is nog onvoldoende.
Zo blijkt randapparatuur zoals printers, scanners, camera´s en netwerkschijven steeds uitgerust te zijn met webservers, die het mogelijk maken de apparaten op afstand, via internet te benaderen. Een aanzienlijk aantal merken blijkt standaard onbeveiligd te zijn, waardoor ze voor iedereen, waar ook ter wereld toegankelijk zijn. Het opstellen van een basisrichtlijn heeft tot doel eisen en verplichtingen te formuleren ten behoeve van de ontwikkeling van nieuwe hard- en software producten, ten einde tijdens de productiefase van een hard- of software component een minimaal beveiligingsniveau te bewerkstelligen. Hierdoor vermindert de kwetsbaarheid van de uit deze componenten geassembleerde systemen, of wordt het moeilijker om een toch aanwezige kwetsbaarheid van het totaal geassembleerde systeem te gebruiken om de componenten ervan te beïnvloeden.
Op deze wijze kan op grote schaal een zeker minimaal beveiligingsniveau bereikt worden zonder afhankelijk te zijn van de te installeren beveiligingen door de gebruikers.
Wie is verantwoordelijk: *de minister van EZ*, in samenwerking met belangengroeperingen. Planning is nog niet aan te geven.

Internationale aandacht voor optimale beveiliging nucleaire installaties
Nederland werkt op internationaal niveau intensief mee om nucleair terrorisme te voorkomen. Daarvoor zet Nederland zich op internationaal/bilateraal niveau in om een optimale beveiliging van nucleaire installaties en radioactieve stoffen / bronnen te bevorderen. Op deze manier kan gezorgd worden voor voorkoming of wegneming van de bron van de dreiging/incident en verlaging van de kans op ontstaan, ontwikkeling of verspreiding van de dreiging/incident.
De Nuclear Security Summit (NSS) die in 2014 door Nederland wordt georganiseerd, vervult daarin een leidende rol. De NSS heeft expliciet tot doel te komen tot een betere beveiliging van nucleair materiaal en installaties, samen met de betrokken 53 landen en 4 internationale organisaties. Deze vertegenwoordigen samen meer dan 95 procent van het wereldwijde nucleaire materiaal.
Het International Atomic Energy Agency (IAEA) heeft in dialoog met de lidstaten een aanbeveling gedaan voor beveiliging van nucleaire installaties, beveiliging van transporten van nucleair materiaal, en opsporing (INFCIRC/225 rev 5). Tevens biedt het

IAEA International Physical Protection Advisory Services (IPPAS) aan, waarbij landen een advies kunnen aanvragen waarmee zij de beveiliging van hun installaties kunnen verbeteren. Het is van belang dat Nederland aandacht vraagt voor het bevorderen van de toepassing hiervan. Transparantie, internationaal vertrouwen en een daadwerkelijke verbetering van internationale beveiliging zijn redenen voor het verbeteren van deze capaciteit.
De maatschappelijke opbrengst van het verbeteren van de internationale beveiliging is verhoogde (inter)nationale veiligheid, internationaal vertrouwen, verbeterde internationale afstemming en samenwerking.
Wie is verantwoordelijk: *De ministers van BZ en EZ*.